Senate Fiscal Agency
P. O. Box 30036
Lansing, Michigan 48909-7536

BILL ANALYSIS

Telephone: (517) 373-5383
Fax: (517) 373-1986
TDD: (517) 373-0543

Senate Bill 309 (Substitute S-5 as reported)
Sponsor: Senator Shirley Johnson
Committee: Judiciary

CONTENT

The bill would amend the Identity Theft Protection Act to provide for notification of people whose personal information contained in a database was acquired by an unauthorized person; and to establish a civil fine for failure to give the required notice, as well as misdemeanor penalties for certain violations. The bill would take effect 180 days after it was enacted.

Under the bill, if a person or agency that owned or licensed data included in a database discovered a security breach, or received notice of a security breach from a person or agency that maintained the database, the person or agency that owned or licensed the data would have to notify each resident of Michigan whose personal information was accessed and acquired by an unauthorized person, including information accessed and acquired in encrypted form by a person with unauthorized access to the encryption key. The bill also would require a person or agency that maintained a database to give notice of a security breach to the owner or licensor of the data.

The notification requirements would apply unless the person or agency determined that the security breach had not or was not likely to cause substantial loss or injury to, or result in identity theft with respect to, one or more Michigan residents. After providing the required notice, the person or agency would have to notify each consumer reporting agency that compiles and maintains files on consumers on a nationwide basis.

A financial institution that met certain Federal requirements for customer notice, and a person or agency that complied with the Federal Health Insurance Portability and Accountability Act, would be considered to be in compliance with the bill.

A person that provided notice of a security breach when a breach had not occurred, with the intent to defraud, would be guilty of a misdemeanor punishable by up to 30 days' imprisonment and/or a maximum fine of $1,000. A person who failed to provide a required notice could be ordered to pay a civil fine of up to $1,000 for each failure. The Attorney General or a prosecuting attorney could bring an action to recover a civil fine. A person's aggregate liability for civil fines for multiple violations from the same security breach could not exceed $2.5 million.

The bill also would require a person or agency that maintained a database that included personal information regarding multiple individuals to destroy any data that were removed from the database and that the person or agency did not retain elsewhere for another purpose not prohibited by law. A knowing or intentional violation of this requirement would be a misdemeanor punishable by up to 30 days' imprisonment and/or a maximum fine of $1,000 for each violation.

In addition, the bill would prohibit a person from distributing an advertisement or making any other solicitation that misrepresented to the recipient the occurrence of a security breach that could affect the recipient. A person also could not distribute an advertisement or make any other solicitation that was substantially similar to a notice required under the bill or by Federal law, if the form of that notice were prescribed by State or Federal law, rule, or regulation. A violation would be a misdemeanor punishable by up to 30 days' and/or a maximum fine of $1,000 for each violation.

The bill's provisions regarding notice of a security breach would preempt local ordinances and regulations.

MCL 445.63 et al. Legislative Analyst: Patrick Affholter

FISCAL IMPACT

Date Completed: 11-30-06 Fiscal Analyst: Lindsay Hollander
Stephanie Yu